CLAIMS

Sub a2

I claim:

1. A method for limiting simultaneous copies of content material , comprising:

communicating a copy of the content material to a receiving device ,

communicating a security challenge to the receiving device when the copy of the content material is communicated to the receiving device , and

receiving a security response, based on the security challenge, from the receiving device when the copy of the content material is removed from the receiving device .

2. The method of claim 1, further including

verifying a certification of the receiving device before communicating the copy of the content material to the receiving device .

3. The method of claim 1, further including

maintaining a count of the simultaneous copies of the content material , including:

incrementing the count when the copy of the content material is communicated to the receiving device , and

decrementing the count when the security response is received from the receiving device , and

wherein

communicating the copy of the content material is dependent upon the count of the simultaneous copies.

4. The method of claim 1, further including:

generating a random number, and

encrypting the random number via a public key of a public-private key pair that is associated with the receiving device to form the security challenge, and

wherein

the security response includes the random number.

5. The method of claim 4, further including

verifying a certification of the receiving device before communicating the copy of the content material to the receiving device , and

wherein

the certification of the receiving device includes a public key of the public-private key pair of the receiving device .

6. A check-out/check-in device comprising:

a catalog controller that is configured to provide a limited number of simultaneous copies of content material to one or more receiving devices,

an encrypter that is configured to provide a security challenge to a receiving device of the one or more receiving devices when the catalog controller provides a copy of the content material to the receiving device , and

a return verifier that is configured to:

receive a security response from the receiving device when the copy of the content material is removed from the receiving device , and

notify the catalog controller whether the security response corresponds to an appropriate response to the security challenge.

7. The check-out/check-in device of claim 6, further including

a certification verifier that is configured to verify a certification of the receiving device , and

wherein

the catalog controller is further configured to provide the content material in dependence upon the certification of the receiving device .

8. The check-out/check-in device of claim 6, wherein

the catalog controller is further configured to maintain a count of the simultaneous copies of the content material ,

wherein,

the catalog controller is configured to:

increment the count when the copy of the content material is communicated to the receiving device , and

decrement the count when the security response is received from the receiving device , and

provide the copy of the content material in dependence upon the count of the simultaneous copies.

9. The check-out/check-in device of claim 6, wherein

the encrypter is configured to encrypt a random number via a public key of a public-private key pair that is associated with the receiving device to form the security challenge, and

the return verifier is configured to compare the security response to the random number to determine whether the security response corresponds to the appropriate response to the security challenge.

10. The check-out/check-in device of claim 9, further including

a certification verifier that is configured to verify a certification of the receiving device , and

wherein

the catalog controller is further configured to provide the content material in dependence upon the certification of the receiving device , and

the certification of the receiving device includes a public key of the public-private key pair of the receiving device .

11. A receiving device that receives content material and a corresponding security challenge from a check-out/check-in device , comprising:

a memory that is configured to store the content material and the corresponding security challenge, and

a security device that is configured to:

erase the content material from the memory , and

communicate a security response to the check-out/check-in device , based on the security challenge that is associated with the content material .

12. The receiving device of claim 11, wherein

the security device is further configured to communicate a certification of the receiving device to the check-out/check-in device to enable the check-out/check-in device to provide the content material to the receiving device .

13. The receiving device of claim 11, wherein

the security device includes:

a decrypter that decrypts the security challenge via a private key of a public-private key pair that is associated with the receiving device to form the security response.

14. The receiving device of claim 13, wherein

the security device is further configured to communicate a certification of the receiving device to the check-out/check-in device to enable the check-out/check-in device to provide the content material to the receiving device , and

the certification of the receiving device includes a public key of the public-private key pair of the receiving device .